**RISK MANAGEMENT-INFORMATION SECURITY**

1. **INTRODUCTION:**

Banks deal with public money and therefore, trust is the most important pillar of the banking business. While trust may be considered synonymous with banking, security is also considered equally important. The concept and perception of security in banking has, over a period of time, changed drastically, in tandem with changes in the way banking business is conducted. Now a days, banks maintain their assets more in digitized rather than physical form, carry out their transactions over technology enabled platforms/applications and communicate through electronic modes. The banking business does not face any growth impediments because of physical, geographical or product/knowledge-related boundaries as technology has come to their aid. There are newer products and channels of delivery. Networked environment has enabled delivery of banking services at the doorstep of the customer. Anywhere, anytime banking with core banking and newer delivery channels viz., ATM, online banking, mobile banking etc. have provided convenience of banking to the customer and more and more people are now relying upon the convenience and ease of use of Internet banking services in their business as well as daily life. But, this has also resulted in enhanced customer expectations about efficient delivery of services with the highest level of security. Growth of business, customer satisfaction and retention of customers’ loyalty, therefore, depend on the highest quality of service coupled with the state of the art security features.

Information and the knowledge based on it have increasingly become recognized as ‘information assets’, which are vital enablers of business operations. It is therefore, absolutely crucial for any organisation to provide adequate levels of protection to these assets. Reliable information is even more critical for banks, as banks are purveyors of money in physical and digital form and hence information security is a vital area of concern.

Robust information is at the heart of risk management processes in a bank. Inadequate data quality is likely to induce errors in decision making. Data quality requires building processes, procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. The fundamental attributes supporting data quality include accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability. The data quality provided by various applications depends on the quality and integrity of the data upon which that information is built. Entities that treat information as a critical organizational asset are in a better position to manage it proactively. Information security not only deals with information in various channels like spoken, written, printed, electronic or any other medium but also information handling in terms of creation, viewing, transportation, storage or destruction .This is in contrast to IT security which is mainly concerned with security of information within the boundaries of the network infrastructure technology domain. From an information security perspective, the nature and type of compromise is not as material as the fact that security has been breached. It is therefore, imperative for Bank Managements to establish an effective information security risk governance framework as a part of the overall Corporate Governance Framework so that the Banks develop and maintain a comprehensive information security programme.

1. **BASIC PRINCIPLES OF INFORMATION SECURITY:**

The basic principles of information security are as under:

1. ***Confidentiality:*** Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network.The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms like Hacking, Phishing, Vishing, Email-spoofing, SMS spoofing, and sending malicious code through email or Bot Networks, as discussed earlier.
2. ***Integrity:*** In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when he/she is able to modify his own salary in a payroll database, when an employee uses programmes and deducts small amounts of money from all customer accounts and adds it to his/her own account (also called salami technique), when an unauthorized user vandalizes a web site, and so on. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.
3. ***Availability:*** For any information system to serve its purpose, the information must be Available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DoS) and distributed denial-of service (DDoS) attacks.
4. ***Authenticity:*** In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.
5. ***Non-repudiation***: In law, non-repudiation implies one's intention to fulfill one’s obligations under a contract / transaction. It also implies that a party to a transaction cannot deny having received or having sent an electronic record. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation. In addition to the above, there are other security-related concepts and principles when designing a security policy and deploying a security solution. They include identification, authorization, accountability, and auditing.
6. ***Identification:*** Identification is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorization and accountability. Providing an identity can be typing in a username, swiping a smart card, waving a proximity device, speaking a phrase, or positioning face, hand, or finger for a camera or scanning device. Proving a process ID number also represents the identification process. Without an identity, a system has no way to correlate an authentication factor with the subject.
7. ***Authorization:*** Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. If the specific action is allowed, the subject is authorized. Else, the subject is not authorized.
8. ***Accountability and auditability:*** An organization’s security policy can be properly enforced only if accountability is maintained, i.e., security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject’s identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the identification. Thus, human accountability is ultimately dependent on the strength of the authentication process. Without a reasonably strong authentication process, there is doubt that the correct human associated with a specific user account was the actual entity controlling that user account when an undesired action took place.
9. **INFORMATION SECURITY GOVERNANCE:**

Information security governance consists of the leadership, organizational structures and processes that protect information and mitigation of growing information security threats like the ones detailed above.

Critical outcomes of information security governance include:

* Alignment of information security with business strategy to support organizational objectives
* Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
* Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved
* Optimisation of information security investments in support of organizational objectives

It is important to consider the organisational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

A comprehensive security programme needs to include the following main activities:

* Development and ongoing maintenance of security policies
* Assignment of roles, responsibilities and accountability for information security
* Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
* Classification and assignment of ownership of information assets
* Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security
* Ensuring security is integral to all organizational processes
* Processes to monitor security incidents
* Effective identity and access management processes
* Generation of meaningful metrics of security performance
* Information security related awareness sessions to users/officials including senior officials and board members
1. **ORGANIZATIONAL STRUCTURE, ROLES AND RESPONSIBILITIES:**
2. **BOARDS OF DIRECTORS/SENIOR MANAGEMENT:**

The Board of Directors is ultimately responsible for information security. Senior Management is responsible for understanding risks to the bank to ensure that they are adequately addressed from a governance perspective. To do so effectively requires managing risks, including information security risks, by integrating information security governance in the effectiveness of information security governance is dependent on the involvement of the Board/senior management in approving policy and appropriate monitoring of the information security function.

The major role of top management involves implementing the Board approved information security policy, establishing necessary organizational processes for information security and providing necessary resources for successful information security. It is essential that senior management establish an expectation for strong cyber security and communicate this to their officials down the line. It is also essential that the senior organizational leadership establish a structure for implementation of an information security programme to enable a consistent and effective information security programme implementation apart from ensuring the accountability of individuals for their performance as it relates to cyber security.

Given that today’s banking is largely dependent on IT systems and since most of the internal processing requirements of banks are electronic, it is essential that adequate security systems are fully integrated into the IT systems of banks. It would be optimal to classify these based on the risk analysis of the various systems in each bank and specific risk mitigation strategies need to be in place.

1. **INFORMATION SECURITY TEAM/FUNCTION:**

Banks should form a separate information security function/group to focus exclusively on information security management. There should be segregation of the duties of the Security Officer/Group dealing exclusively with information systems security and the Information Technology Division which actually implements the computer systems. The organization of the information security function should be commensurate with the nature and size of activities of a bank including a variety of e-banking systems and delivery channels of a bank. The information security function should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. While the information security group/function itself and information security governance related structures should not be outsourced, specific operational components relating to information security can be outsourced, if required resources are not available within a bank. However, the ultimate control and responsibility rests with the bank.

1. **INFORMATION SECURITY COMMITTEE:**

Since information security affects all aspects of an organization, in order to consider information security from a bank-wide perspective a steering committee of executives should be formed with formal terms of reference. The Chief Information Security Officer would be the member secretary of the Committee. The committee may include, among others, the Chief Executive Officer (CEO) or designee, chief financial officer (CFO), business unit executives, Chief Information Officer (CIO)/ IT Head, Heads of human resources, legal, risk management, audit, operations and public relations.

A steering committee serves as an effective communication channel for management’s aims and directions and provides an ongoing basis for ensuring alignment of the security programme with organizational objectives. It is also instrumental in achieving behaviour change toward a culture that promotes good security practices and compliance with policies.

Major responsibilities of the Information Security Committee, inter-alia, include:

* Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within a bank’s risk appetite
* Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving standards and procedures
* Supporting the development and implementation of a bank-wide information security management programme
* Reviewing the position of security incidents and various information security assessments and monitoring activities across the bank
* Reviewing the status of security awareness programmes
* Assessing new developments or issues relating to information security
* Reporting to the Board of Directors on information security activities

Minutes of the Steering Committee meetings should be maintained to document the committee’s activities and decisions and a review on information security needs to be escalated to the Board on a quarterly basis.

1. **CHIEF INFORMATION SECURITY OFFICER (CISO):**

A sufficiently senior level official, of the rank of GM/DGM/AGM, should be designated as Chief Information Security Officer, responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating the security related issues / implementation within the organization as well as relevant external agencies. The CISO needs to report directly to the Head of Risk Management and should not have a direct reporting relationship with the CIO. However, the CISO may have a working relationship with the CIO to develop the required rapport to understand the IT infrastructure and operations, to build effective security in IT across the bank, in tune with business requirements and objectives.

1. **CRITICAL COMPONENTS OF INFORMATION SECURITY:**
2. ***Policies and procedures:***

Banks need to frame Board approved information security policy supported with relevant standards, guidelines and procedures need to be framed and appropriate measures/practices need to be identified and implemented keeping in view the business needs.

1. ***Risk Assessment:***

Risk assessment is the core competence of information security management and must include, for each asset within its scope, identification of the threat/vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance or contractual perspective.

**3) *Inventory and information/data classification:***

Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset.

By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules/requirements for each class, it is possible to define the level of access controls that should be applied to each information asset.

**4) *Defining roles and responsibilities:***

All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management. Some of the major ones include:

1. Information owner
2. Application owner
3. User manager
4. Security Administrator
5. End user

**5) *Access Control:***

An effective process for access to information assets is one of the critical requirements of information security. Internal sabotage, clandestine espionage or furtive attacks by trusted employees, contractors and vendors are among the most serious potential risks that a bank faces. Current and past employees, contractors, vendors and those who have an intimate knowledge of the inner workings of the bank’s systems, operations and internal controls have a significant advantage over external attackers. A successful attack could jeopardise customer confidence in a bank’s internal control systems and processes. Hence, access to information assets needs to be authorised by a bank only where a valid business need exists and only for the specific time period that the access is required.

**6) *Information security and information asset life-cycle:***

Information security needs to be considered at all stages of an information asset’s life-cycle like planning, design, acquisition and implementation, maintenance and disposal. Banks need to apply systematic project management oriented techniques to manage material changes during these stages and to ensure that information security requirements have been adequately addressed.

**7) *Personnel security:***

Application owners grant legitimate users access to systems that are necessary to perform their duties and security personnel enforce the access rights in accordance with institution standards. Because of their internal access levels and intimate knowledge of financial institution processes, authorized users pose a potential threat to systems and data. Employees, contractors, or third-party employees can also exploit their legitimate computer access for malicious or fraudulent reasons. Further, the degree of internal access granted to some users can increase the risk of accidental damage or loss of information and systems. Risk exposures from internal users include altering data, deleting production and back-up data, disrupting/destroying systems, misusing systems for personal gain or to damage the institution, holding data hostage and stealing strategic or customer data for espionage or fraud schemes. It is, therefore, important to have a process to verify job application information for all new employees and additional background and credit checks based on the sensitivity of a particular job or access level.

**8) *Physical security:***

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. As such, it is important to mitigate the physical security risks through zone-oriented implementations and by having proper risk assessment and environmental controls.

**9) *User Training and Awareness:***

It is acknowledged that the human link is the weakest link in the information security chain. Hence, there is a vital need for an initial and ongoing training and information security awareness programme. The programme may be periodically updated keeping in view changes in information security, threats/vulnerabilities and/or the bank’s information security framework. There needs to be a mechanism to track the effectiveness of training programmes through an assessment/testing process designed on testing the understanding of the relevant information security policies, not only initially but also on a periodic basis. At any point of time, a bank needs to maintain an updated status on user training and awareness relating to information security and the matter needs to be an important agenda item during Information Security Committee meetings.

**10) *Incident management:***

Incident management is defined as the process of developing and maintaining the capability to manage incidents within a bank so that exposure is contained and recovery achieved within a specified time objective. Incidents can include the misuse of computing assets, information disclosure or events that threaten the continuance of business processes. An effective incident management framework for preventing, detecting, analyzing and responding to information security incidents is therefore, required to be implemented.

**11) *Application Control and Security:***

Financial institutions have different types of applications like the core banking system, delivery channels like ATMs, internet banking, mobile banking, phone banking, network operating systems, databases, enterprise resource management (ERP) systems, customer relationship management (CRM) systems, etc., all used for different business purposes. Then these institutions have partners, contractors, consultants, employees and temporary employees. Users usually access several different types of systems throughout their daily tasks, which makes controlling access and providing the necessary level of protection on different data types difficult and full of obstacles. This complexity may result in unforeseen and unidentified holes in the protection of the entire infrastructure including overlapping and contradictory controls, and policy and regulatory noncompliance. Banks, therefore, need to implement proper application control and risk mitigation measures.

**12) *Migration controls:***

A documented Migration Policy indicating the requirement of roadmap/ migration plan / methodology for data migration (which includes verification of completeness, consistency and integrity of the migration activity and pre and post migration activities along with responsibilities and timelines for completion of same) is required to be put in place to take care of data integrity, completeness, confidentiality, consistency and continuity.

**13) *Implementation of new technologies:***

Banks need to carry out due diligence with regard to new technologies since they can potentially introduce additional risk exposures. A bank needs to authorise the large scale use and deployment in production environment of technologies that have matured to a state where there is a generally agreed set of industry-accepted controls and robust diligence and testing has been carried out to ascertain the security issues of the technology or where compensating controls are sufficient to prevent significant impact and to comply with the institution’s risk appetite and regulatory expectations. A formal product approval process incorporating, inter-alia, security related aspects and fulfilment of relevant legal and regulatory prescriptions should also be in place for all new business products introduced by the bank.

**14) *Encryption:***

There are two types of encryption – Symmetric and Asymmetric.

**Symmetric encryption** is the use of the same key and algorithm by the creator and reader of a file or message.

**Asymmetric encryption** lessens the risk of key exposure by using two mathematically related keys, the private key and the public key. When one key is used to encrypt, only the other key can decrypt. Therefore, only one key (the private key) is required to be kept secret.

Typical areas or situations requiring deployment of cryptographic techniques, given the risks involved, include transmission and storage of critical and/or sensitive data/information in an ‘un-trusted’ environment or where a higher degree of security is required, generation of customer PINs which are typically used for card transactions and online services, detection of any unauthorised alteration of data/information and verification of the authenticity of transactions or data/information. Since security is primarily based on the encryption keys, effective key management is crucial.

**15) *Data security:***

Banks need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

**16) *Vulnerability Assessment:***

Banks need to scan for vulnerabilities and address discovered flaws proactively to avoid a significant likelihood of having their computer systems compromised because any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain.

**17) *Establishing on-going security monitoring processes:***

A bank needs to have robust monitoring processes in place to identify events and unusual activity patterns that could impact on the security of IT assets. The strength of the monitoring controls needs to be proportionate to the criticality of an IT asset. Alerts would need to be investigated in a timely manner, with an appropriate response determined.

**18) *Security measures against Malware:***

Malicious software is an integral and a dangerous aspect of internet based threats which target end-users and organizations through modes like web browsing, email attachments, mobile devices, and other vectors. Malicious code may tamper with a system's contents, and capture sensitive data. It can also spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block their execution. Banks should, therefore, have proper preventive and detective/corrective controls at the host, network, and user levels to protect against malicious codes by using layered combinations of technology, policies and procedures and training.

**19) *Patch Management:***

A documented standards / procedures for patch management needs to be in place to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

**20) *Change Management:***

Banks need to establish a change management process covering all types of change. For example, upgrades and modifications to application and software, modifications to business information, emergency ‘fixes’, and changes to the computers/networks that support the application.

**21) *Audit trails:***

Banks needs to ensure that audit trails exist for IT assets satisfying the banks business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution.

**22) *Information security reporting and metrics:***

Banks need to have security monitoring arrangements to provide key decision-makers and Senior Management/Board of Directors with an informed view of aspects like the effectiveness and efficiency of information security arrangements, areas where improvement is required, information and systems that are subject to an unacceptable level of risk, performance against quantitative, objective targets, actions required to help minimize risk (e.g., reviewing the organization’s risk appetite, understanding the information security threat environment and encouraging business and system owners to remedy unacceptable risks).

**23) *Information security and Critical service providers/vendors:***

Banks use third-party service providers in a variety of different capacities like an Internet service provider (ISP), application or managed service provider (ASP/MSP) or business service provider (BSP). Management should evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives and institute effective third-party controls to enhance the ability of the bank to achieve its control objectives.

**24) *Network Security:***

Protection against growing cyber threats requires multiple layers of defenses, known as defense in depth. As every organization is different, this strategy should therefore be based on a balance between protection, capability, cost, performance, and operational considerations. Some of the important network protection devices are

1. Firewalls,
2. Intrusion Detection Systems
3. Network Intrusion Prevention Systems
4. Quarantine
5. DNS Placement

**25) *Remote Access:***

Banks may sometimes provide employees, vendors, and others with access to the institution’s network and computing resources through external connections. Those connections are typically established through modems, the internet, or private communications lines. Remote access to a bank’s provides an attacker with the opportunity to manipulate and subvert the bank’s systems from outside the physical security perimeter. The management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. These devices should be strictly controlled.

**26) Distributed Denial of service attacks(DDoS/DoS):**

Banks providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilization which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyze anomalies in networks and systems. Banks should, therefore, install and configure network security devices appropriately for reasonable preventive/detective capability.

**27) *Implementation of ISO 27001 Information Security Management System:***

Commercial banks should implement Information Security Management System (ISMS) best practices for their critical functions/processes with the best known ISMS as described in ISO/IEC 27001 and ISO/IEC 27002 and related standards published jointly by ISO and IEC.

**28) *Wireless Security:***

Wireless network includes all wireless data communication devices like personal computers, cellular phones, PDAs, etc. connected to a bank’s internal networks. Wireless networks security is a challenge since the wireless data communication devices do not have well-defined perimeters or well-defined access points and unauthorized monitoring and denial of service attacks can be performed without a physical wire connection. Further, unauthorized devices can potentially connect to the network, perform man-in-the- middle attacks, or connect to other wireless devices. To mitigate those risks, wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications. The banks using a wireless network should, therefore, carefully evaluate the risks involved and implement appropriate additional controls.

**29) *Business Continuity Considerations:***

Events that trigger the implementation of a business continuity plan may have significant security implications. Depending on the event, some or all of the elements of the security environment may change. Different tradeoffs may exist between availability, integrity, confidentiality, and accountability, with a different appetite for risk on the part of management. It is, therefore, imperative that the business continuity plans are reviewed as an integral part of the security process.

**30) *Information security assurance:***

**a) Penetration Testing:**

Penetration testing is defined as a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system’s or organization’s resistance to such an attack. Penetration testing is performed to uncover the security weaknesses of a system and to determine the ways in which the system can be compromised by a potential attacker.

**b) Audits**

Auditing compares current practices against a set of policies/standards/guidelines formulated by the institution, regulator including any legal requirements. Bank management is responsible for demonstrating that the standards it adopts are appropriate for the institution. Audits should not only look into technical aspects but also the information security governance process.

**c) Assessment**

An assessment is a study to locate security vulnerabilities and identify corrective actions. An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks.

A bank should manage the information security risk management framework on an ongoing basis as a security programme following project management approach, addressing the control gaps in a systematic way.

**31) *General information regarding delivery channels:***

Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking should be issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. A customer should not be forced to opt for services in this regard. Banks should provide clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services. When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank should ensure that customers have sufficient instruction and information to be able to properly utilize them. Banks should sensitize customers on the need to protect their PINs, security tokens, personal details and other confidential data to raise security awareness levels. Banks need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks.

1. **EMERGING TECHNOLOGIES AND INFORMATION SECURITY:**

The security concerns in respect of the technologies like virtualisation and cloud computing which have been emerging increasingly of late also need to be considered by Banks.

1. **Virtualization**

Of late, the trend in the data center has been towards decentralization, also known as horizontal scaling because centralized servers were seen as too expensive to purchase and maintain. However, decentralization’s application sandboxes have a high annual maintenance cost and lower efficiency. Virtualization is a modified solution between centralized and decentralized deployments. Instead of purchasing and maintaining an entire computer for one application, each application is given its own operating system, and all those operating systems reside on a single piece of hardware. This provides the benefits of decentralization, like security and stability, while making the most of a machine’s resources.

**Challenges of Virtualization**

a. Compatibility and support

b. Licensing

c. Staff training

d. Reliability

**(b) Cloud Computing**

Cloud computing refers to computing environment owned by a company which is shared with client companies through web-based service over Internet which hosts all the programs to run everything from e-mail to word processing to complex data analysis programs. Service may include software, platform or infrastructure. At the backend, cloud computing can make use of virtualization and grid computing. In grid computing, networked computers are able to access and use the resources of every other computer on the network.

**Cloud Computing Concerns**

The biggest concerns about cloud computing are security and privacy.

1. **IMPLEMENTATION OF RECOMMENDATIONS OF THE WORKING GROUP ON INFORMATION SECURITY, ELECTRONIC BANKING, TECHNOLOGY RISK MANAGEMENT AND CYBER FRAUDS:**

The Banking Industry has been conscious of the challenges to Security and appreciable efforts are being made by all the stakeholders in the context, viz. Governments, Regulators, banks and technology providers. In this regard, the Reserve Bank of India issued Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds in 2011, which were based on the report submitted by the working group constituted by RBI under the Chairmanship of Shri. G. Gopalakrishna, Executive Directror, RBI.

The guidelines are not “one-size-fits-all” and the implementation of these recommendations need to be risk based and commensurate with the nature and scope of activities engaged by banks, the technology environment prevalent in the bank and the support rendered by technology to the business processes. Banks with extensive leverage of technology to support business processes were required to implement all the stipulations outlined in the circular. Banks were also required to conduct a formal gap analysis between their current status and stipulations as laid out in the guidelines and put in place a time-bound action plan to address the gap and comply with the guidelines.

The guidelines are fundamentally expected to enhance safety, security, efficiency in banking processes leading to benefits for banks and their customers. The measures suggested for implementation are not static. Banks need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

1. **CONCLUSION:**

In the IT enabled banking environment, information security is of paramount importance because it involves tremendous risk that can result in huge business and financial losses which can also assume international dimensions. As it is often said, in a chain, it is the weakest link that is the most vulnerable. Therefore, it is not only important to *ab initio* take care of the information security risks but we also need to make sure that the information security risk management process adopted by us is continuously benchmarked against the international standards. There has to be a paradigm shift in the perception about security in banking and the top management’s response to the same. It is important for banks to realize that they have a vital role and responsibility to ensure that appropriate risk management measures are in place to avoid frauds, losses and business disruption.

It may be noted that the real challenge in this environment goes beyond merely providing additional technology solutions and increasingly complex security layers, and translates into providing secured banking while balancing the same against customer convenience requirements, which puts the regulators and security implementers on the horns of a dilemma. For a Bank, while the challenges to information security are stiff and are increasing by the day, being alive to threats is of the highest importance. This also involves resources - human and monetary, attitude and aptitude and a continuous monitoring and review of the information security management processes.